Math 412/512 Assignment 2

Due Thursday, October 1

1) Prove that there are infinitely many prime numbers.

2) (#12, Chapter 2) Show that if $\gcd(a, b) = 1$, then $\text{lcm}(a, b) = ab$. In general, show that

$$\text{lcm}(a, b) = \frac{ab}{\gcd(a, b)}.$$

3) (#9, Chapter 3) Prove that multiplication on $\mathbb{Z}_m$ as defined in the text is well-defined.

4) Enumerate $\mathbb{Z}_m = \{[0]_m, [1]_m, [2]_m, [3]_m, \ldots, [m-1]_m\}$.

a) Prove that the product of all *nonzero* elements in $\mathbb{Z}_m$ is equal to $[0]_m$ if and only if m is composite UNLESS m is equal to 4!

b) Prove that if n is relatively prime to m, then $\exists s \in \mathbb{N}$, $[n]_m[s]_m = [1]_m$.

c) If p is prime, prove that the product of all *squares* of nonzero elements in $\mathbb{Z}_p$ is equal to 1.

d) (Extra Credit) If p is prime, show that the product of all nonzero elements in $\mathbb{Z}_p$ is equal to $[p-1]_p$. I will not accept written solutions; you must present your solution to me in my office on the board.

5) (#5, Chapter 4) Let n be an odd integer and consider the polynomial

$$\Phi_{n+1} = \frac{x^{n+1} - 1}{x - 1} = x^n + x^{n-1} + \cdots + x + 1.$$

Use the Root Theorem 4.3 to argue that Φ_{n+1} has a linear factor. We call Φ_{n+1} a **cyclotomic polynomial**.

6) We've seen some similarities between $\mathbb{Z}$ and $\mathbb{Q}[x]$. Now, let's explore some differences.

a) By successively adding one to itself, we obtain all of $\mathbb{N}$. Taking all additive inverses, we have all of $\mathbb{Z}$ except zero. Show that there is no polynomial $p(x)$ such that adding $p(x)$ to itself and taking additve inverses gives all of $\mathbb{Q}[x]$ except zero.

b) (#13, Chapter 4) We say that $p(x) \in \mathbb{Q}[x]$ has a multiplicative inverse if there exists $q(x) \in \mathbb{Q}[x]$, $p(x)q(x) = 1$. In $\mathbb{Z}$, there are only two numbers with multiplicative inverses. Prove that there are infinitely many elements in $\mathbb{Q}[x]$ with multiplicative inverses, and these are precisely the constant functions.